Performance Work Statement (PWS)
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
Defense Biometric Identification System (DBIDS) and Identity Matching Engine for Security and Analysis (IMESA) Support
ORDER ID - ID03180056003

1.0 INTRODUCTION

The Defense Manpower Data Center requires Subject Matter Expertise (SME) and Program Management support for the Physical Security and Law Enforcement program to include Physical Access Control Systems (PACS), Defense Biometric Identification System (DBIDS) and Identity Matching Engine for Security and Analysis (IMESA).

2.0 BACKGROUND

2.1 Military installations across the Department of Defense (DOD) utilize outer and inner perimeter rings with varying levels of security to control physical access to secure areas. The Defense Biometric Identification System (DBIDS) Business Rules Committee (BRC) has requested that DMDC analyze the architecture of the current Base Services and/or totality of the DBIDS 5 application in managing identities and their respective unique profiles. DMDC will work with the BRC to facilitate the execution of the requirements referenced in this document. The enterprise goal is to integrate these findings with DBIDS for optimization and data quality. This new solution must be cost effective and provide a scalable approach that can be implemented across the DOD enterprise and identified in future development roadmaps.

2.2 DMDC supports major programs and initiatives within the DOD and maintains the largest archive of personnel, manpower, training, security and financial data within the DOD. Specifically, DMDC's data supports decision making to determine the eligibility for both physical and logical access to military installations and DOD systems worldwide. DMDC's physical and logical access systems include the Defense Biometric Identification Service (DBIDS) system which identifies DOD affiliated persons through the use of ID cards, base passes, and biometric attributes and grants access based on their privileges in accordance with their purpose, fitness and status.

2.3 DMDC has developed the Identity Matching Engine for Security and Analysis (IMESA) physical security concept, designed to continuously evaluate the fitness of persons who have attempted and are attempting to access DOD installations. The IMESA solution uses DoD, Federal, State, and local authoritative data sources to look for derogatory information and send alerts to authorized and connected Physical Access Control Systems (PACS) so individuals who may pose terrorist, criminal, and/or security threats may be detained and adjudicated. The IMESA solution covers all DoD installations and any person seeking to gain physical access to them and enhances the security of DoD personnel. Personnel data in the IMESA solution comes from two places: the Defense Enrollment Eligibility Reporting System (DEERS) and the Local Population Database (LPDB). IMESA pulls from DEERS information on individuals who possess credentials authorized to facilitate access. The LPDB provides the IMESA solution with data on individuals who possess a credential authorized to facilitate access to installations that are not contained in DEERS; this includes non- DoD Federal Personal Identity Verification (PIV) credentials, approved DoD PIV-Interoperable credentials, local DoD installation issued

cards/passes, Transportation Worker Identification Credentials (TWIC), Veteran Health Identification Card (VHIC) and other authorized credentials.).

3.0 SCOPE

The Contractor shall provide the personnel and management necessary to support planning, designing, sustaining, developing, and implementing Physical Security and Law Enforcement (PSLE) programs and systems.

4.0 REQUIREMENTS

The Contractor shall:

4.1 DBIDS Sustainment Development

The contractor shall provide the personnel and support necessary for development of all current product services and continue integration into DBIDS 5 (D5), and also provide documentation and creation of training material, processes, and procedures in support of the requirements in Section 4. The contractor shall be responsible to create/sustain/maintain a production integration system that can handle all D5 services as defined by the D5 Roadmap and approved requirements.

4.1.1 Product Enhancement

4.1.1.1 Maintenance of Existing Applications

4.1.1.2 Support the software maintenance of all portions of the D5 and IMESA software applications to include the following:

- Routine and emergency bug fixes
- Routine software changes caused by dependent third-party library updates
- Minor software changes caused by policy changes
- Depending on number of components requiring updates, per approved project plan

4.1.1.3 Support the update and refinement of features as maintained in the government approved business requirements.

4.1.1.4 Utilize most current approved requirements documentation at the start of the Period of Performance. (Government furnished).

4.1.1.5 All software changes to D5 will be confirmed in a production staging environment with participating beta installations for a period of no less than 14 days before being pushed to production except for an emergency, a Change Request shall be approved, signed off via email and directed by the government.

4.1.1.6 Confirmation (e-mail with documentation) shall include a confirmation of data integrity between CONUS DBIDS, IOLS, and PDR, at a minimum, and sign off from DBIDS and IMESA Government Product and Program Managers.

4.1.2 Reports

4.1.2.1 Investigations Report

Contractor shall develop a report to display all personnel who have generated a dossier on a particular individual. Report user shall be able to search for report by requesting operator or by investigation subject via DBIDS ID. Report shall detail the where the ORI (Originating Agency Identifier) was requested from and the timestamp the report was generated. Report shall not be restricted by date range. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.2 Operator Transactions Report

Contractor shall develop a report to display a list of operators who have scanned at the local installation and sort them by number of transactions recorded. The guard scans shall be grouped by base and ACP (Access Control Point). The report shall show the total per guard, base at which they are scanned, then total scans per base. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.3 Installation Health Report

Contractor shall develop report to display usage rate of issuances compared to scanned frequency, and other health metrics. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.4 Issuance by Operator Report

Contractor shall develop report to display all credentials issued by a particular operator at an installation. The following fields shall be returned after report is generated: operator, credential type, and total. Report shall be filterable by date range, base, and credential type. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.5 Enhanced Screening Watch list Reports

Contractor shall develop report to display events and remarks from the Enhanced Screening Watchlist within a given date range. The following fields shall be returned after report is generated: subject name, photo (if exists), address, email, identifier, aliases, any remarks, and total event history. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.6 Base Access Control Report by Credential Type

Contractor shall develop report to display scans at a base grouped by credential type within a given date range. The following fields shall be returned: date, name, direction, access decision, reason, action, operator name, and credential type. The report shall show a total number of each in the header of report. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.7 Exception to Policy (ETP) Report

Contractor shall develop report to display all instances where an ETP was applied to an individual. This report shall be base specific and ETPs applied will be grouped by operator who applied the ETP. The following fields shall be returned when the report is generated, date the ETP was applied, subject of ETP's name, any remarks associated with ETP status, begin date and end date of ETP status, and total number of each in the header of report. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.8 Vetting Adjudication Aggregate History Report

Contractor shall develop report to display adjudications by aggregate (approved, denied, and access type) over a date range. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.9 Forecast Re-adjudication Report

Contractor shall develop report to display individuals who will need to be re-adjudicated within a certain date range (30, 60, or 90 days). The report will be timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.3 Data Warehousing

Contractor shall build out an initial Data Warehouse in Structured Query Language (SQL) Server Analysis Services.

- Contractor shall build out star schema using fact and dimension tables for the access transaction data. The contractor shall conduct analysis on what fact and dimension tables need to be created.
- The Contractor shall create SQL Server Integration Services jobs to migrate data from online transaction processing (OLTP) to the Online Analytical Processing (OLAP).

4.1.3.1 Enhance SQL Server Reporting Services (SSRS)

Contractor shall modify the enrollment workstation and web portal to be compatible with dynamic SSRS reports. Contractor shall build out enhanced SSRS environment.

4.1.3.2 Power Business Intelligence (BI)

Contractor shall conduct analysis on whether Power BI would be usable in a DOD production environment to give Service points of contact enhanced business intelligence capabilities.

4.1.4 Base Service Modeling and Performance Enhancements

Contractor shall fix technical debt acquired from legacy DBIDS components remaining from data migration, and old versions of IMESA. This is necessary to deliver new features and resolve DMDC mandated cybersecurity/security/coding compliance issues going forward.
Specific areas to fix are:

- Sponsorship for base access instead of sponsoring credentials
- Consolidation of credential models
- Access permissions applied to the individual rather than affiliation

4.1.5 Facial Recognition

4.1.5.1 Contractor shall implement functionality during enrollment at the registration workstation to use facial recognition as a way to assist in the disambiguation of potential matches of biographic data.

4.1.5.2 Contractor shall implement functionality to allow a credential to be scanned, pull up the latest picture on file in DBIDS or IMESA / Defense Enrollment Eligibility Reporting System (DEERS) and determine if the person presenting the credential at the registration workstation matches the photo on file.

4.1.6 Vetting Module

4.1.6.1 Contractor shall integrate IMESA real-time queries and display eXtensible Markup Language (XML) returns. Due to historical IoLS identity limitations, there are often multiple IoLS profiles for a single

person in DBIDS. This will allow the vetting officer to determine if there are any statuses that are not being merged and take appropriate action.

4.1.6.2 Contractor shall assist Government in determining feasibility of integrating with NCIC-CE (National Crime Information Center – Continuous Evaluation).

4.1.6.3 Contractor shall assist Government in determining feasibility of integrating with JPAS/JVS (Joint Personnel Adjudication System/Joint Verification System), Interpol, DCII (Defense Central Index of Investigations), and other DBIDS regions.

4.1.7 Identity Proofing Module

4.1.7.1 Contractor shall add identity breeder document capture in workstation and integrate with Government designated document scanner once determined.

4.1.7.2 Contractor shall perform a proof of concept on 10-print live scan.

4.1.7.3 Integrate NLETS (National Law Enforcement Telecommunications System) driver's license query and passport query by displaying the XML return by NLETS.

DBIDS Additional Development (OPTIONAL)

4.2.1 Mobile Enrollment and Credentialing (OPTIONAL)

4.2.1.1 Upon execution of OPTIONAL CLIN, the Contractor shall have 12 months to implement core infrastructure to support a multiyear effort to implement a secure, multi-platform mobile enrollment and credentialing system detailed below under 4.2.1.

4.2.1.2 Develop and Maintain Sponsor Website.

- The sponsor website shall allow an authorized user to send invitations for installation access and provide preliminary identity proofing of the invitees.

4.2.1.3 Website Authentication

- The website shall require Common Access Card (CAC) authentication for users affiliated with the DOD, Personal Identity Verification (PIV) authentication for users affiliated with another U.S. government agency, and email/password for DBIDS card holders.

4.2.1.4 Access Invitations

- The sponsor shall have the ability to send a single access invitation consisting of invitee name, email address, mobile phone number (optional). The sponsor must include the name of the installation, where access is needed, the date range access is required, and a reason for access or comments text block.
- The sponsor shall have the ability to send an event or group invitation (e.g. Basic Military Training invitee list). The invitation must include a group/event name, the name of the installation where access is needed, the date range access is required, a reason for access or comments text block, and one or more invitees which shall consist of name, email address, and mobile phone number (optional).
- Upon sponsor submission of the invitation, the system shall send out an email and an optional text to the invitee containing instructions on how to start the enrollment process. The email shall

contain a link that, when opened on a mobile device, shall redirect to the appropriate app store to download the DBIDS Mobile Credential App.

- If the invitee is already known to the system, the system shall additionally send a notification to the DBIDS Mobile Credential App on the invitee's phone.

4.2.1.5 Invitee Identity Proofing

- Once the invitee(s) a sponsor has invited have finished their mobile enrollment, the sponsor shall be notified (by email, optionally text, and within the Sponsor Website) that he needs to verify the invitee's identity.
- The sponsor shall view the invitee "selfie" photo taken and confirm, deny, or indicate he is unsure whether the photo matches the person invited.

4.2.1.6 Mobile Credential.

- The mobile credential application shall be used for identity enrollment into DBIDS and, upon a positive adjudication by a vetting officer; it shall be used as an access credential. The token for the access credential shall be derived using a one-time password (OTP) algorithm.
- The mobile credential must operate on both iOS and Android devices.
- Authentication
    - The mobile credential user shall have the option to authenticate with email/password, Facebook ID, or Google ID (including Facebook and Google would help with identity proofing).
- Account
    - The user must setup an account that is tied to the email address provided by the sponsor.
    - The user must verify possession of the email address used by clicking on a link in an email where the link contains a temporary token that ties back to the account created.
    - During account creation, the user may select whether to use an email/password, or acceptable single sign on methods as an authentication mechanism.
    - The user can select to enable Touch ID, Face ID, or Pin for subsequent logins on that mobile device.
- Enrollment
    - The user must start the enrollment process by capturing their face from multiple angles.
    - The software shall use facial detection software to ensure that appropriate data is collected.
    - The user must enter a primary identifier number per the DBIDS system requirements.
    - The user must take a photo of the front and back of his primary identify proofing credential. This is limited to REAL ID (i.e. Government ID, Standard driver's license, etc) or Passport.
    - The software shall extract the user's name, date of birth (DOB), aliases, and address from the credential.
    - The software shall extract the face photo from the identity proofing credential provided and send both that photo and the mobile capture photo to a web service. The web service shall perform facial recognition between the two photos and determine if the person is the same.
    - The user must take a photo of the front and back of a secondary proofing document.
    - The user shall have the option to manually enter his name, DOB, address(es), phone #('s) if that information could not be captured via the credential scan.
    - If the identity information is entered manually, the system must extract identity information from the primary and secondary proofing document using OCR, and ensure that the 3 identity sources match.
    - The software shall maintain an event log of all actions performed during the enrollment.

- The software shall submit the user's completed enrollment to the sponsor and vetting officer for additional proofing and vetting.

4.2.1.7 Identity Services

4.2.1.7.1 Facial Recognition

- The identity web service shall accept a photo of a credential containing a facial photo and a photo of a person, perform facial recognition between the two photos, and return a match result.

4.2.1.7.2 Counterfeit Credential Detection

- The identity web service shall accept photos of REAL ID and Passport credentials and use machine learning/AI to detect a counterfeit.
- In order to perform the machine learning, a training set of the supported credentials (valid and invalid) must be generated / acquired.

4.2.1.7.3 DBIDS Identity Matching Engine

- The identity web service shall run each identity profile against an identity matching algorithm to ensure the profile does not already exist in DBIDS. The algorithm shall include the following:
  - Diacritic characters shall match to their base glyphs (e.g. ä matches a, ĉ matches c)
  - String similarity matching using the damerau-levenshtein algorithm (to catch minor misspellings).
  - Address matching.
  - Identifier matching.
  - Biometric matching (fingerprints, iris, facial).
  - Alias name matching.
  - Email matching.
  - Phone number matching.
  - Common nickname matching (i.e. Richard with also match on Rick, Rich, etc. even though those aliases were not provided).
  - Each match shall receive a score from 0 to 100.
  - Each matching category shall receive a weight.
  - The identity matching engine shall return a weighted score based on the comparison between the two identity profiles.

4.2.1.8 Mobile Enrollment and Credential Validation

- Contractor shall work with stake holders to identify and document additional requirements necessary to complete follow-on work required for full implementation of mobile enrollment and validate and confirm mobile credential information.

4.2.2 IdAM(Identity Access Management) Solution (OPTIONAL) - Upon execution of OPTIONAL CLIN and acquisition of IdAM solution the Contractor shall have 12 months to implement the IdAM solution.

4.2.2.1 Any changes identified by the Government shall require the Contractor to determine changes to requirements, costing model, and potential conflicts with previously proposed solution, and added to the approved project plan.

4.2.2.2 The IdM (identity management) solution shall monitor the regional DBIDS database and upon the detection of an operator account being created, shall start an in-processing workflow. The IdM solution shall be the platform for in-processing, provisioning, account maintenance, continuous evaluation of, and out-processing for DBIDS users in order to stay compliant with account lifecycle management policies.

4.2.2.3 This solution shall satisfy the two-factor authentication requirement mandated by DoD.

4.2.2.4 This solution shall enable the transition to the PIV-Auth cert as mandated by DoD.

4.2.2.5 The IdM solution shall monitor the regional DBIDS database and upon the detection of an operator account being created, shall start an in-processing workflow.

4.2.2.6 The in-processing workflow shall consist of DD-2875 workflow which involves the user's supervisor and a government approver.

4.2.2.7 Upon approval of the 2875, the account shall be provisioned into Active Directory and other supplemental DBIDS user stores.

4.2.2.8 Additional in-processing workflows can be requested by Government and requirements be established by Contractor.

4.2.2.9 Contractor shall provide access to Government requested users to provide auditing and governance of 2875s.

4.2.2.10 The IdM solution shall continuously monitor the regional DBIDS database for any adverse statuses or account termination requests and if detected, shall start an out-processing workflow.

4.2.2.11 The out-processing workflow shall consist of disabling the user's account in Active Directory and any other supplemental DBIDS user stores.

4.2.2.12 The IdM solution shall implement a bulk processing task to transition all user accounts from a DoD identity cert authentication to the PIV-Auth cert.

4.2.2.13 All DBIDS application authentication shall be consolidated to use the IdAM solution access manager.

Device Configuration Updates (OPTIONAL)

4.2.2.14 Contractor shall augment to include ability for hardware middleware, access control devices, and ACWs (Access Control Workstations) to communicate back to a web service hosted at the regional data center and write execution context information.

4.2.2.15 Contractor shall create a report that displays the connectivity status of the various devices stated above. The report shall be grouped by base. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.2.2.16 Contractor shall create a method for setting the configuration values such as mapping the IP address to ACP (Access Control Point) Mapping, Gate assignment, timeout values, access code settings, etc.

4.2.2.17 This method should accommodate the following Access Control Devices: Lantronics, iCam7, enhanced secure pedestrian gate (ESPG), and the Cheetah AVG.

4.3 **IMESA Enhancements**

4.3.1 Provide development support based on policy updates provided by DMDC, OUSD(I) and other stakeholders.

4.3.2 Develop tool for internal use to visualize all relevant information of an individual based on LPEDI or DoD EDI

4.3.3 Review existing ICD (Interface Control Document) and propose changes to government stakeholders on a quarterly basis in a formal report with proposed changes.

4.3.4 DBIDS integration development with IMESA changes will occur per approved project plan.

4.3.5 Add an error for partial ADR (Active Data Repository in DEERS) information on inquire by identity when DOB is missing

- Add an indicator to display a person status
- *Add credentials used for registration*
- Allow more than one credential to be added to an identity

4.3.4 Review and report existing architecture to determine where potential data integrity issues could occur based on multiple supported ICDs, multiple PACS (Physical Access Control System), and multiple regions.

4.3.5 Develop standardized method to merge identities determined to be duplicate and expose the necessary information to participating PACS and recommendation to implement their own merge protocols.

4.3.6 Work with government stakeholders to identify policy on exposing additional functionality not documented in the official ICD for beta development and testing purposes by participating PACS.

4.3.7 Add the ability to search all completed cases without the need to load all cases into the GUI

4.3.8 Allow the user with a specific role to select which IMESA application they would like to view (e.g., Dashboard, multi-threat alert center (MTAC), law enforcement officers (LEO)

4.3.9 Create new user roles for the IMESA application, IMESA Managers and LEO roles

4.3.10 Update Matching Algorithm

4.3.11 Allow PACS to confirm receipt of data alert when needed

4.3.12 Build a LEO application for external users

4.3.13 Develop functionality allowing users to export Dashboard reports to Excel

The following paragraphs apply to the sections that immediately follow regarding terrorist screening database (TSDB) Phase II, national sex offender registry (NSOR) Integration, violent person file (VPF) Integration, and interstate identification index (III) POC:

4.3.14 The research and development for the NSOR and VPF will proceed in parallel with the research for the III, and each can succeed independently. This parallel structure is necessary given the greater level of risk associated with the III research compared with the NSOR and VPF.

4.3.15 The Initial Capabilities Document development and Interoperability Layer Service (IoLS) development are two sequential tasks that will also proceed in parallel with the NSOR and VPF, but which must complete prior to the NSOR and VPF completing.

4.3.16 The TSDB portion requires technical work such as identity resolution / matching, database design, software development, website development, PKI-enablement, workflow processing, technical writing, and program management.

4.3.17 TSDB Phase II

- Contractor shall build upon the work done in the previous phase by making minor enhancements to the TSDB match review capability and implementing person-oriented reporting for NCIC-origin security alerts, researching and developing a way to eliminate duplicate alerts for the same person and offense as present in current alert-based reporting. Contractor shall research applicable criminal justice regulations to ensure that this reporting is implemented in accordance with the same.
- Contractor shall test all enhancements in accordance with TSDB testing rules, and the reports submitted to the Government. The granular reporting functionality will be spot checked by having two installations manually tally the results of their security alerts and matching those tallies against the generated report.

4.3.18 NSOR Integration

- Contractor shall design and develop the required enhancements to the IMESA matching engine workflow to identify potential matches between all registered cardholders and the NSOR with varying degrees of data quality and match points.
- Contractor shall make the required updates to the Interface Control Document that describes the technical underpinnings of the interface between the installation physical access control systems and IMESA to support the transmission of NSOR originated alerts to the Installations.
- Contractor shall develop a capability to transmit alerts derived from changes in person data from NSOR through IoLS to the IMESA-connected PACS, including IMESA's ability to receive, through loLS, any necessary PACS acknowledgements of those alerts.

4.3.19 VPF Integration

- Contractor shall design and develop the required enhancements to the IMESA matching engine workflow to identify potential matches between all registered cardholders and the VPF with varying degrees of data quality and match points.
- Contractor shall make the required updates to the Interface Control Document that describes the technical underpinnings of the interface between the installation physical access control systems and IMESA to support the transmission of VPF originated alerts to the Installations.
- Contractor shall develop a capability to transmit alerts derived from changes in person data from VPF through IoLS to the IMESA-connected PACS, including IMESA's ability to receive, through loLS, any necessary PACS acknowledgements of those alerts.

4.3.20 III POC

- Contractor shall design and develop a capability to monitor and provide alerts for any changes in III data on all registered cardholders. Contractor shall coordinate with the FBI, criminal justice information system (CJIS), and related groups and boards as necessary to research and design this process.
- Contractor shall make the required updates to the Interface Control Document that describes the technical underpinnings of the interface between the installation physical access control systems and IMESA to support the transmission of III originated alerts to the Installations.

- Contractor shall develop a capability to transmit alerts derived from changes in person data from III through IoLS to the IMESA-connected PACS, including IMESA's ability to receive, through loLS, any necessary PACS acknowledgements of those alerts.

4.3.21 DoDM 5200.08, Vol 3

- Contractor shall implement changes required per DoDM 5200.08, Vol 3.

4.4 IMESA Integration with DBIDS

4.4.1 DBIDS shall be the system used for initial demonstration of any modifications to IMESA.

4.4.2 DBIDS integration development with IMESA changes will occur per approved project plan.

4.4.3 Except in the event of an emergency Change Request, any change to IMESA shall be confirmed in a production staging environment with participating beta installations for a period of no less than 14 days before being pushed to production.

4.4.4 Confirmation shall include a confirmation of data integrity between CONUS DBIDS, IOLS, and PDR, at a minimum.

4.4.5 Confirmation shall include sign off from both product owners - DBIDS and IMESA Government Product and Program Managers.

4.4.6 Integrate TSDB Phase II with DBIDS

Contractor shall implement TSDB Phase II functionality to include the capability of storing silent encounters received from IMESA.

4.4.7 Integrate NSOR with DBIDS

Contractor shall work with Interoperability Layer Service (IoLS) to analyze requirements to demonstrate PACS ability to ingest NSOR data and properly display access recommendation and mitigate concerns from the customer base regarding policy of NSOR data.

4.4.8 Integrate VPF with DBIDS

Contractor shall work with IoLS to analyze requirements to demonstrate PACS ability to ingest VPF data and properly display access recommendation and mitigate concerns from the customer base regarding policy of VPF data.

4.4.9 Integrate III POC with DBIDS

Contractor shall work with IoLS to analyze requirements to demonstrate PACS ability to ingest III data and properly display access recommendation and mitigate concerns from the customer base regarding policy of III data.

4.4.10 DoDM 5200.08, Vol 3

Contractor shall support necessary changes introduced in DoDM 5200.08, Vol 3 by assisting Government in deriving requirements for implementation in DBIDS and IMESA.

4.5 Baseline DBIDS Operations/Production Support (approximately 300 bases/installations connected to the CONUS RDC (Regional Distribution Center)

4.5.1 The contractor shall perform the maintenance and administration of the following items to support the DBIDS and Labs infrastructure as listed below.

4.5.2 Support, maintain and administer the clients, servers and applications as outlined in Appendix 2.

4.5.3 Maintain operating system - Weekly Patching / STIGS / Updates

- Maintain up to date IA approved OS image for future servers

4.5.4 Monitor capacity and performance issues and provide upgrade support and recommendations prior to end of life status.

4.5.5 Review the 5 year planning cycle provided by DMDC for all DBIDS hardware on a semi-annual basis identifying any potential compatibility issues.

4.5.6 Review the 5 year planning cycle provided by DMDC for all DBIDS software dependencies on a semi-annual basis identifying any potential compatibility issues.

4.5.7 Provide business architecture support by ensuring system design diagrams remain up-to-date, update documents and views based on configuration changes, evolving requirements, data flows and security enhancements, use SPARX or other tool as provided by government.

4.5.8 Maintain NoSQL Databases - DBA

4.5.9 Maintain Relational/non-relational Databases - DBA for SQL Relational Database Administration

4.5.10 Perform Data Quality Analysis – Respond to inquiries from Product and Program Managers when there are data quality or data integrity issues that need to be resolved.

4.5.11 Respond/perform Misc. Adhoc Requests - Requests may include: troubleshooting, ACW (Access Control Workstation) for individual installation, networking, OCONUS RDC administration guidance, and other requests outside of Tier 3 helpdesk support. The Government anticipates an average of 30 per year, ad hoc requests from DMDC and its customers. Provide monthly ad hoc report status.

4.5.12 Migration of Training Environment

- Contractor shall facilitate deployment of training environment into identified/approved cloud provider.
- Contractor shall facilitate the creation and administration of Active Directory forest and subdomains as needed.
- Contractor shall facilitate the creation and administration of Windows and Linux servers as needed to deploy the DBIDS stack.
- Contractor shall ensure compliance with all DoD IA STIGS as per FedRAMP+ solution.
- Contractor shall deploy data stores as needed.
- Contractor shall deploy web servers as needed, including load balancers and reverse proxies.

- Contractor shall provide demonstration environment. However, production implementation is dependent on Government licensure.
- Contractor shall deploy any dev required development dependency in order to support the build and deploy pipeline.
- Contractor shall automate the deployment of the software in the training environment using DevOPs pipeline.

4.5.13 DBIDS Monthly Statistics Rollup

Contractor shall provide an updated monthly DBIDS brief with relevant statistics for number of transactions, statuses, dbids credentials and visitor passes created, registrations, etc., as well as, updated application screenshots

4.5.14 Training Material

Contractor shall provide updated Training Material (i.e. User Manuals, Training Manuals, Training Videos) and make available on the DBIDS marketing site and the wiki per government direction.

4.6 DBIDS 5 Worldwide Tier 3 Help Desk

4.6.1 Provide Tier 3 helpdesk support 0800-1700 PST on site in the DoD Center.

4.6.2 Establish and maintain the Tier 3 helpdesk log with problem, date received, estimated completion date and priority. The Government product owner shall assign priorities during the weekly IPR.

4.6.3 All logged items that remain be reported in the monthly SMR and reported to the product owner.

4.6.4 Performance requirement summary for Tier 3

Requirement	Delivery
Triage tier 3 tickets for resolution	2-hours of receipt of ticket
Notify customer of the status of the ticket	4-hours of receipt of ticket
Update root cause of ticket	8-hours of receipt of ticket
75% of all tickets resolved	6-hours of receipt of ticket
100% of all tickets resolved	3-business days

1. Notify Government lead at if unresolved after 3 business days.

2. Provide updates to Government lead as requested.

3. Provide weekly report of Tier III tickets to Government lead to include cumulative status year to date by month.

4. Identify and provide recommendation to recurring issues.

5. Performance requirement summary for Tier 3 is only applicable to tickets received during 0800-1700 PST, Monday-Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The clock for any ticket received outside of these hours will start next business day at 0800 PST.

6. Performance requirements summary apply to tickets once assigned to DBIDS DMDC West Queue (Tier 3).

7. These requirements are applicable to tickets that involve work to be performed by the GCE DBIDS Tier 3 team. Any ticket that requires work to be performed external to the GCE DBIDS team is outside of this performance requirement scope. However, GCE will provide ticket status to Government lead if not resolved within 3 business day and when applicable, continue to provide status within weekly IPR.

4.7 Full 24 hour Regional Distribution Centers (RDC) Support. (OPTIONAL CLIN)

4.7.1 Expands help desk Support to 24/7 coverage in the DoD Center.

4.7.2 Expands help desk Support to include OCONUS RDC system administrative support**.**

4.8 Provide Cyber Security Support

4.8.1 Provide administrative and logistical support for the operations environment of DMDC physical and logical access control systems and applications supporting the DoD goal of strengthening cyber capabilities and expertise to ensure reliability while countering and preventing threats.

4.8.2 Provide technical support to planning, execution, analysis and performance of decision processes, applications and systems such as architecture, vulnerability, methodologies, operations monitoring and data structures.

4.8.3 Document and Implement all NIST RMF controls. For DBIDS and IMESA (PSLE CORE environment) assist with ATO accreditation documentation, Army Certificate of Net worthiness, Air Force Ability to Connect and other Service documents as determined by government approved project plan.

4.8.4 Support DMDC Cyber Hardening Initiative. All applications (DBIDS, IMESA) must be scanned by the specified tools (Fortify, SonaType and WebInspect), POA&M must be provided to the Cyber Hardening team for the issues identified by those tools.

4.9 Provide Security Infrastructure

4.9.1 Prepare documentation as required by NIST (Risk Management Framework) RMF to submit to the contractor that performs the Assessment and Authorization (A&A) of systems.

4.9.2 Participate in Incident response, security auditing, privacy act auditing, and monitoring of applications as directed.

4.9.3 Evaluate security technology as it applies to authentication, authorization, and auditing of in scope applications, databases and systems & provide recommendations to enhance security or comply with regulations

4.9.4 Provide Information Assurance (IA) Support; perform code reviews of developed code using code analysis tools as directed by cyber security.

4.9.5 Security Compliance & Patch Management. Cybersecurity is directed by the DMDC Cybersecurity Branch. Security compliance and patch management is a crucial element in systems administration and IT operations. IT security planning, implementation, and compliance is integral to all work performed at DMDC and, therefore, participation is a shared responsibility. The contractor is responsible for continuing to maintain security compliance support and performing patching. Patch Management is one of the major features of the enterprise suite. It encompasses researching, testing and deploying patches for remediation of vulnerabilities identified by security tools managed by the Cybersecurity Branch.

4.9.6 Perform Information Assurance Vulnerability Management (IAVM) & Situational Awareness Report (SAR) compliance patching on all servers, workstations and all other IAVM & SAR applicable assets on both the SIPRNET and NIPRNET networks. Remediation is to be completed according to IAVM or SAR guidelines as appropriate. Report IAVM or SAR patch compliance to the Cybersecurity Branch according to reporting guidelines. Deliver initial IAVM & SAR within 30 days of award; update with changes thereafter

4.9.7 All physical and logical access control IT assets must meet Security Technical Implementation Guides (STIGs) compliance prior to operating on the DMDC or Global Information Grid (GIG) network. Implement, apply and maintain STIG configuration to all IT assets. Deviations from STIG configuration setting must follow the DMDC STIG Deviation process and be approved by the Cybersecurity Branch.

4.9.8 Apply vendor supported security patches on a continuous and timely basis per DoD and DMDC policy. Patches should be applied within two weeks of release unless otherwise directed by government. Support third-party software updates and apply definitions to all applicable DMDC IT assets (e.g., network, servers and workstations).

4.9.9 All new IT assets built under this contract and baseline images must go through the DMDC Pre-production process and approved by Cybersecurity prior to operation in a production environment.

4.9.10 Install, configure, and test patches and changes required by Information Assurance Vulnerability Management (IAVM) issuances, vendor patches and STIG configuration items. Implement all necessary changes to Enterprise software and equipment in accordance with the suspense date articulated by the Cybersecurity Branch.

4.9.11 Remediate software vulnerabilities and system misconfigurations for physical and logical access control systems and applications identified in the DMDC vulnerability management tool managed by Cybersecurity Branch

4.9.12 Provide a Plan of Actions and Milestones (POAM) for remediation actions that cannot be accomplished by the Cybersecurity Branch assigned completion date.

4.9.13 Provide a STIG Deviation/Non-Compliance report for system configuration items that cannot be accomplished by the Cybersecurity Branch assigned completion date within 30 days of award and monthly thereafter.

4.9.14 Develop, implement and provide the government a Patch Management Plan that shall test and remediate vulnerabilities within the DoD timeline (currently TASKORD 13-067).

4.9.15 Correct STIG configuration items within 3 days identification by the Cybersecurity Branch.

4.9.16 Gather and collect data to support reporting of IAVM and (Federal Information Security Management Act) FISMA compliance reports and Access and Authorization (A&A).

4.9.17 Ensure all IT assets have the required cybersecurity monitoring tools (e.g., tripwire agent, HBSS agent) installed and operational in accordance with DoD and DMDC policy.
***Responsible for the up to date and compliant build, configuration and operations of the DISA provided Host Based Security System (HBSS) across all platforms associated to the OCONUS DBIDS environment and associated reporting requirements.

4.9.18 All software or hardware patches, updates, firmware must come from the DoD patch repository. Exceptions must be approved by the Cybersecurity Branch prior to engagement.

4.9.19 Provide applications services that are in compliance with and support DoD PKI or Intelligence Community (IC) policies.

4.9.20 Provide Security solutions for CE tools that meet confidentiality, data integrity, authentication, and non-repudiation requirements. Solutions shall comply with (NIST, Federal Information Processing Standards (FIPS) standards, and DoD or IC standards.

4.9.21 Coordinate patches or changes that require system or application down time with the Government and schedule during allotted maintenance hours.

4.10 Program Management

4.10.1 Provide business processes that support the integration of activities, maximizing communications among stakeholders while focusing on quality, timeliness, cost efficiency, and accuracy in the delivery of required services.

4.10.2 Business Analysis. Maintain existing government approved business requirements and add additional requirements per the scope of this PWS.

4.10.3 Identify and understand the business problem and the impact of the proposed solution on the organization's operations. Implement training methods and provide training as required.

- Provide onsite training as required for major system revisions (DBIDS 3.1 to DBIDS 5 for example)

4.10.4 Document the complex areas of project scope, objectives, and added value or benefit expectations, using an integrated set of analysis and modeling tools.

4.10.5 Evaluate customer business needs, thus contributing to strategic planning of fiscal, information systems and technology directions.

4.10.6 Work with major development and production support teams during preliminary installation and testing of new products and services.

4.10.7 Design and develop high quality business solutions; construct models, process, data, and workflow, develop business architecture: as-is and to-be models and analyze and manage requirement risk.

4.10.8 Structure requirements for traceability, prioritize requirements and draft requirement specifications.

4.10.9 Facilitate an annual Business Rules Committee and DBIDS Users Group among the appropriate stake holders as identified by the Product and Program Managers of DBIDS and IMESA. Capture and integrate all artifacts derived from the meetings.

4.11 Project Management

4.11.1 IT project managers support all phases of the software development lifecycle and shall follow the DMDC Application Development Process to manage a variety of projects, to include new development, sustainment, infrastructure projects and projects transitioning from and to DMDC infrastructure.

4.11.2 Implement a comprehensive project management approach to include technical management, schedule management, cost management, personnel management, and communication management.

4.11.3 Utilize project management best practices such as those defined in the Project Management Body of Knowledge.

4.11.4 Provide experience in multiple software development project management methodologies, to include waterfall and Scrum/Agile methodologies.

4.11.5 Allocate resource estimates to specific tasks and deliverables or sets of deliverables, including system releases.

4.11.6 Ensure all project management activities are conducted using standardized processes, to include a repeatable SDLC.

4.11.7 Provide project management support to infrastructure projects, to include system maintenance, system upgrades, migrations, and new infrastructure planning and implementation.

4.11.8 Develop project plans and follow industry standard management principles, to include risk management, critical path, resource allocation, stakeholder communication, and milestone reviews.

4.11.9 Assist in evaluating impacts to current schedules and alternative allocations of resources to minimize disruption/impacts introduced by new/changing requirements. Provide updated project schedules within 14 days of changes.

4.12 Provide Plans, Reports and Documentation

4.12.1 Provide Product Documentation and Reports

4.12.2 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

4.12.3 Conduct Weekly In-Progress Reviews (IPR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

4.12.4 Problem Notification Report (PNR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

4.12.5 Provide a Quality Control Plan (QCP)

4.12.6 DMDC is committed to a highly interactive relationship between quality control by the Contractor and quality assurance by the government recipient of services. This relationship shall be achieved through a Prevention Based Quality System dedicated to ensuring the best possible products and services. A copy of the comprehensive written QCP shall be submitted to the Contracting Officer (KO) and Contracting Officer's Representative (COR) within 5 working days when changes are made thereafter. The Contractor shall provide their final QCP no later than (NLT) 10 calendar days after contract award.

4.12.7 The Contractor's quality system shall demonstrate its prevention-based outlook by meeting the objectives stated in the PWS throughout all areas of performance and shall be developed to specify the Contractor's responsibility for management and quality control actions to meet the terms of the contract. The Contractor's QCP shall be incorporated into and become part of this Order after the plan has been accepted by the Government. The Contractor's QCP shall be maintained throughout the life of the Order and shall include the Contractor's procedures to routinely evaluate the effectiveness of the plan to ensure the Contractor is meeting the performance standards and requirements of the Order.

4.12.8 RISK MANAGEMENT PLAN

4.12.9 The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this contract in a Risk Management Plan. The Risk Management Plan shall be delivered no later than (NLT) 10 calendar days after contract award.

4.12.10 WORK BREAKDOWN STRUCTURE (WBS)

Submit a final detailed Work Breakdown Structure (WBS). The WBS shall detail the decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables in accordance with the statement of work. Define each of the tasks required to complete the work, identify individual responsibilities, and describe output, timelines for completion and performance standards. The Work Breakdown Structure shall identify final completion dates and progress milestones for tasks and provides a basis for monitoring and evaluation contractor work. The WBS shall be delivered no later than (NLT) 10 calendar days after contract award.

4.12.11 Participate in Kick Off Meeting

This meeting provides an introduction between the Contractor and Government personnel who will be involved with the contract and shall aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. This meeting is not a substitute for the contractor to fully understand the work requirements at the time offers were submitted nor is it to be used to alter the final agreement arrived at in any negotiations leading to contract award. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Kick Off Meeting to the COR. Kick off meeting minutes shall be documented by the contractor and delivered to the Government within 3 business days of the Kick off meeting.

5 DELIVERABLES

THE CONTRACTOR SHALL SUBMIT A DRAFT VERSION OF EACH DELIVERABLE AND THE GOVERNMENT WILL PROVIDE WRITTEN ACCEPTANCE, COMMENTS AND/OR CHANGE REQUESTS, IF ANY, IN ACCORDANCE WITH PWS SECTION 5.0. THE CONTRACTOR SHALL MAKE ANY CORRECTIONS AND SUBMIT THE FINAL DELIVERABLE, IN ACCORDANCE WITH THE DATES LISTED IN THE FOLLOWING TABLE AND IN ACCORDANCE WITH PWS SECTION 5.0. The Government will provide written acceptance, comments and/or change requests, if any, within ten (10) work days from Government receipt of the draft deliverable (if necessary), and sign off on the deliverable check sheet for the final draft of the deliverable within three (3) work days after the due date for submission into ITSS. After three days if not approved, the deliverable is deemed acceptable. The work products and reports shall be delivered in accordance with dates listed in the following table:

Deliverables for DBIDS/IMESA	PWS Reference	Date Due/Frequency
System design documents.	4.5.7	Architecture update prior to production release
Ad hoc Reports	4.5.11	provide status NLT 5th duty day of the preceding month
Hardware & software compatibility List	4.5.5 &4.5.6	Semi-annually
DBIDS reports (Monthly DBIDS statistics Rollup)	4.5.13	NLT 5 business day of the month
DBIDS Program Management Plan and Schedule	4.4, 4.10	Within 30 days of award; updates within 10 days of change in plans
IMESA Program Management Plan and Schedule	4.3, 4.10	Within 30 days of award; updates within 10 days of change in plans
User Training Documentation and videos of most common functions	4.5.14	update with every release thereafter
Demonstration	4.3.11.5 4.3.12.2 4.3.13.2	per Government Approved Project Plan
Training Manual/User Manual	4.1, 4.5.14	update with every release
RMF and NIST security and risk control documentation	4.8.3, 4.9.1	monthly updates and reviews
IAVM and SAR compliance Report	4.9.6, 4.9.10, 4.9.16	update with changes when appropriate
POAM	4.9.12	update with changes when appropriate
STIG Deviation/Non Compliance Report	4.5.3, 4.9.7, 4.9.13	update with changes when appropriate
Patch Management Plan	4.9.14	Critical vulnerabilities within 7 days of discovery, high

		vulnerabilities within 21 days of discovery, low vulnerabilities within 60 days of discovery.
Monthly Status Report (SMR)	4.12.2	15th of each month
QCP	4.12.5	Within 10 calendar days of award
Risk Management Plan	4.12.9	Within 10 calendar days of award
WBS	4.12.10	Within 10 calendar days of award
Kick Off Meeting Minutes	4.12.11	Within 3 business days of award
Problem Notification Reports	6.5	NLT 5 business days after identification of problem
Travel Reports	10.0	Within 5 business days of completed travel
Weekly IPR	4.12.3	Weekly

6.0 QUALITY ASSURANCE

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ.

6.1 PERFORMANCE STANDARDS

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	METHOD OF SURVEILLANCE
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.	100% inspection

Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.	100% inspection
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.	100% inspection

7.0 CONTRACTOR PERSONNEL

The contractor shall provide qualified personnel under this and ensure they possess the skills, knowledge, training required to ensure satisfactory performance of all services required.

8.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

The Contractor shall follow the requirements identified in the PWS Section 10.8 of the EITS II Base IDIQ.

9.0 CONTRACT ADMINISTRATION

9.1 Contract Type: This contract shall be firm fixed price (FFP).

9.2 Period of Performance: The period of performance (PoP) for this Task Order will be 12 months, with two optional periods of 12 months each.

9.3 Place of Performance: The work under this task will be performed on site at DMDC facilities in Seaside, CA. Any work performed at other locations shall be identified in a formal submission and approved by the Identity Division or equivalent DMDC Government division. Occasional to significant travel may also be required, as noted in PWS Section 10.0-Travel.

9.4 Hours of operation: The contractor is responsible for conducting business between the hours of 6 a.m. to 5 p.m.PT, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task will require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations (if the 24 hour support optional CLIN is exercised).

9.5 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

9.6 Telecommuting/Telework: The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of

the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the contractor. The Contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task order may commence with Contracting Officer and Contracting Officer Representative (COR) approval under the following: Telework requests shall be approved by the Contracting Officer and the Contracting Officer Representative.

9.7 Points of Contact:

DMDC COR
Will be assigned Post Award

GSA Contracting Officer (CO)
Mr. James Purdy
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: James.Purdy@gsa.gov
Tel: (b) (6)

GSA Contract Specialist (CS)
Mr. David Long
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: David.Long@gsa.gov
Tel: 215-446-4597

GSA Contracting Officer's Representative (COR)
Mr. Shail Shah
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Shail.shah@gsa.gov
Tel: 215-446-5858

10.0 TRAVEL

It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR.
All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.0 SECURITY

The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ

In addition, all contractor personnel under this task order shall be fully adjudicated to get a credential and some or all personnel may be required to hold at a minimum a fully-adjudicated and active Secret security clearances. Contractor personnel shall possess these security clearances at Task Order award. The Government may require some or all personnel under this task to hold a Top Secret with SCI security clearance.

12.0 INVOICING

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

13.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf